

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

PROPHET MORTGAGE OPPORTUNITIES, LP,

Plaintiff,

-v-

CHRISTIANA TRUST, a division of Wilmington
Savings Fund Society, FSB, as both Owner Trustee
and Indenture Trustee of RBSHD 2013-1 Trust,

Defendant,

and RBSHD 2013-1 TRUST,

Nominal Defendant.

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #: _____
DATE FILED: 03/11/2024

Case No.: 1:22-cv-09771-MMG

~~{PROPOSED}~~ **PROTOCOL
FOR DISCOVERY OF
ELECTRONICALLY STORED
INFORMATION**

Plaintiff and Defendants (collectively, the “Parties,” and individually, a “Party”) submit this Protocol for Discovery of Electronically Stored Information (hereinafter “Order”) to govern discovery of electronically stored information in this action. This Order will serve as a supplement to Federal Rules of Civil Procedure and any other applicable orders and rules.

A. Definitions

1. **“Requesting Party”** means and refers to the Party that serves a request for the production of Documents.
2. **“Producing Party”** means and refers to the Party upon whom a request for the production of Documents is served.
3. **“Document”** or **“Documents”** means any information or item discoverable pursuant to Federal Rule of Civil Procedure 34(a)(1).
4. **“Document Family”** means a Document and all other Documents that are attached to it, the Document to which other Documents are attached being the “Parent,” and Documents that are attached to the Parent being the “Children.”

5. **“Custodian”** means the individual from whose files the Document originated, or in the case of a Document that originated from a document source not associated with the files of one particular individual, the general source of that Document.

6. **“Electronically Stored Information”** or **“ESI,”** means any Document or Documents stored or transmitted in electronic form.

7. **“Email”** means electronic messages sent using electronic mail protocols (*e.g.*, SMTP).

8. **“E-Message”** means a non-Email form of electronic messaging, including text and group messaging (*e.g.*, Slack, Cisco Jabber, Microsoft Teams, Instant Bloomberg, Google Chat, SMS, MMS, iMessage, Microsoft Lync, WhatsApp, WeChat).

9. **“E-Document”** means a word processing, spreadsheet, presentation or other file (other than Email or E-Messages) stored or transmitted in electronic form.

10. **“Hard-Copy Document”** means any Document existing in paper form at the time of collection.

11. **“Image Format”** means an individual page or pages of a Document that has been converted into a static format. Documents produced as TIFFs are produced in Image Format.

12. **“Native Format”** means and refers to the format of ESI in which it was generated and/or as used by the Producing Party in the usual course of its business and in its regularly conducted activities. For example, the Native Format of an Excel workbook is a .xls or .xlsx file.

13. **“Metadata”** means information about a Document aside from the contents of the Document itself.

14. **“Optical Character Recognition”** or **“OCR”** means the process of capturing text from an image for the purpose of creating a parallel text file that can be associated with the image and searched in a database.

15. **“Hash Value”** is a unique value for a given set of data, similar to a digital fingerprint, that is calculated by a mathematical algorithm and represents the binary content of the data to assist in subsequently ensuring that data has not been modified.

16. “**Confidentiality Designation**” means the confidentiality designation affixed to Documents as defined by, and subject to, the Confidentiality Agreement and Protective Order, or any applicable agreement or stipulation, entered in this matter.

17. “**Searchable Text**” means the text extracted directly from a native Document or generated using OCR from any Document that allows the Document to be electronically searched.

18. “**Load Files**” means electronic files provided with a production set of Documents and images that indicate where individual pages or files belong together as Documents or Document Families used to load that production set into a Requesting Party’s Document review platform.

B. General

1. The Parties commit to cooperate in good faith throughout the pendency of the e-discovery process.

2. Any practice or procedure set forth herein may be varied by agreement of the Parties, which will be confirmed in writing. The Parties will meet and confer to resolve any dispute regarding the application of this Order before seeking Court intervention.

C. Preservation

1. To reduce the costs and burdens of preservation and to ensure proper ESI is preserved, the Parties represent that these data sources are not reasonably accessible because of undue burden or cost, and ESI from these sources will be preserved only to the extent it is ordinarily preserved in the normal course of business. These sources need not be collected, searched, reviewed, or produced, except for good cause shown:

- a. backup systems and/or tapes used for disaster recovery purposes only or that are substantively duplicative of data that is more accessible elsewhere;
- b. systems, server, and network logs;
- c. systems no longer in use that cannot be accessed without undue effort;
- d. automatically saved interim versions of Documents and Emails;
- e. deleted, slack, fragmented, or other data accessible only by forensics;

- f. random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;
- g. on-line access data such as temporary internet files, history, cache, and cookies;
- h. dynamic fields of databases or log files that are not retained in the usual course of business;
- i. voice messages, except for voicemail that is converted to text and forwarded to the recipient's email account; and
- j. Encrypted data/password protected files, where the key or password cannot be ascertained absent extraordinary efforts.

D. Search

1. The Parties agree that in responding to an initial Fed. R. Civ. P. 34 request, or earlier if appropriate, they will meet and confer about methods to search ESI to identify ESI that is subject to production in discovery and filter out ESI that is not subject to discovery.

2. As part of discovery, the Parties agree that they may use keyword searching and/or advanced analytics (i.e., technology-assisted-review ("TAR"), Active Learning, etc.) to help to identify responsive data. The Parties agree to allow sufficient transparency for the Parties to be confident in the process and results and with the goal of limiting the scope of review for production, minimizing the need for motion practice, and facilitating production in accordance with the deadlines set for this matter. Any Party utilizing TAR agrees to disclose information sufficient for the opposing Party to assess the adequacy of the TAR model, including project validation sample sizes, elusion rate, and recall rates.

3. The Parties agree that they will discuss and strive to agree upon appropriate data sources and custodians each Party believes will possess responsive information.

4. The Parties agree that, notwithstanding any conferral, responding Parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own ESI and will execute any reasonable search methodology including but

not limited to TAR tools to produce documents in this litigation. To the extent the Requesting Party believes a methodology is inadequate, the Requesting Party can move the Court for relief, after conferring with the Producing Party in an attempt to resolve the issue without Court intervention.

E. Processing Specifications

1. De-Duplication. The Producing Party shall take reasonable steps to remove Documents identified as duplicative based on MD5 or SHA-1 hash values of the full text of the parent-level Documents, including Email header information, notes, and annotations. Documents within a Document Family shall be considered duplicative of other Documents only if all Documents within each Document's Document Family are duplicative. An Email that includes content in the BCC or other blind copy field shall not be treated as a duplicate of an Email that does not include content in the BCC or other blind copy field, even if all remaining content in the Email is identical. Exact duplicates of Documents retrieved from different Custodians may be considered duplicative despite originating from a different Custodian. A Producing Party shall not use other means to remove duplicate Documents from production (*e.g.*, manual review). The Parties shall timely meet and confer regarding any disputes regarding the de-duplication process.

The Producing Party shall provide a Metadata field "ALLCUSTODIANS" for all Documents, listing the Custodian of the Document if available and all Custodians that possessed or held any duplicate of the Document that was removed through de-duplication. Such de-duplicated documents shall be deemed produced from the files of each such identified Custodian for all purposes in this litigation, including for use at deposition and trial. A Producing Party shall use a uniform description of a particular Custodian across productions. In the event there is no singular Custodian available, the Producing Party shall label the Custodian as the general source of the information. The other Metadata fields, including the To/From/Cc fields, provide the information as to which other Custodians are involved with which documents and communications.

2. Email Threading. The Parties are permitted to use industry standard Email threading tools to remove Emails and their attachments where the contents of the Email and its attachments are wholly included within another Email and its attachments that are not removed.

3. System Files/Application Executable Files. Each Party will use reasonable efforts to filter out common system files and application executable files. Non-user generated files may be removed from review and production using the list of non-user generated files maintained by the National Institute of Standards and Technology (NIST). Additional culling of system files based on file extension may include, but are not limited to: WINNT, LOGS, DRVS, C++ Program File (c), C++ Builder 6 (cpp), Channel Definition Format (cdf), Creatures Object Sources (cos), Dictionary file (dic), Executable (exe), Hypertext Cascading Style Sheet (css), JavaScript Source Code (js), Label Pro Data File (IPD), Office Data File (NICK), Office Profile Settings (ops), Outlook Rules Wizard File (rwz), Scrap Object, System File (dll), temporary files (tmp), Windows Error Dump (dmp), Windows Media Player Skin Package (wmz), Windows NT/2000 Event View Log file (evt), Python Script files (.py, .pyc, .pud, .pyw), and Program Installers. Parties need not produce non-human readable E-Documents, except upon a showing of good cause by the Requesting Party.

4. Embedded Objects. Embedded objects or files (e.g., Excel spreadsheets, Word documents, audio and video files, etc.), shall be extracted, searched and produced consistent with other ESI. Non-substantive embedded files (e.g., MS Office embedded images, email in-line images, logos, etc.), need not be extracted. All extracted embedded files produced shall be produced subject to the same requirements set forth in this Protocol. For production purposes, embedded files shall be identified as attachments to the parent document in which the file was embedded, and load files for such embedded files shall refer to the parent document in which the file was embedded.”

5. Hyperlinked Files. A Producing Party is not required to produce hyperlinked files as part of the same Document Family as the Document containing the hyperlink, provided

however, that upon reasonable and particularized request, a Producing Party will produce or identify such files to the extent it can locate them.

6. Compressed Files. Compression file types (*e.g.*, .CAB, .GZ, .RAR, .TAR, .Z., .ZIP, etc.) shall be decompressed in a manner that ensures a container within a container is decompressed into the lowest uncompressed element resulting in individual files. The container file itself shall not be produced.

7. Searchable Text. Searchable Text must be extracted directly from the native Document unless the Document requires redaction, is an image, or is any other native electronic file that does not contain text to extract (*e.g.*, non-searchable PDFs), in which case Searchable Text shall be created using OCR. Searchable Text shall include all non-privileged comments, revisions, tracked changes, speaker's notes and hidden text. Searchable Text from Email shall include all non-privileged header information that would be visible if the Email were viewed natively including: (1) the individuals to whom the Email was directed, (2) the author of the Email, (3) any recipients copied or blind copied on such Email, (4) the subject line of the Email, (5) the date and time of the Email, and (6) the names of any attachments. Searchable Text shall not contain the Bates number or Confidentiality Designation, to the extent reasonably feasible.

8. Time and Date. When processing ESI, UTC should be selected as the time zone. Producing Parties will process ESI so as to maintain the date/time in the Document's Metadata as it was last saved or last modified by the Custodian or end user, not the date of collection or processing.

9. Exception Files. The Parties will use commercially reasonable efforts to address Documents that present processing or production problems (including encrypted and/or password protected files) ("Exception Files"). Exception Files that are attached to produced Documents will be produced as a Bates-stamped placeholder in Image Format bearing the legend, "This Document was unable to be processed." The Parties will meet and confer regarding requests for the production of the native versions of Exception Files and/or efforts to locate passwords for specifically identified Documents protected by passwords. If the Parties cannot reach agreement

on the handling of Exception Files through the meet and confer process, the matter may be submitted to the Court for resolution.

10. Hard-Copy Documents. Documents that exist only in hard-copy format are to be scanned and produced electronically in Image Format (.TIFF). Reasonable efforts are to be employed to scan the pages of Hard-Copy documents in the same order in which are maintained in the ordinary course of business; to treat pages that are stapled, clipped, or otherwise clearly appear to be part of the same Document as a single Document; and to treat Documents that clearly appear to be separate Documents as separate Documents. Individual pages in notebooks, notepads, or journals shall be considered separate, individual Documents. For Hard-Copy Documents found in folders or other containers with labels, tabs, or other identifying information, such labels and tabs shall be scanned where reasonably practicable. Original Document orientation (*i.e.*, portrait v. landscape) should be maintained. Searchable Text shall be created using OCR.

F. Production Format

The Parties will produce Documents in the format described in **Exhibit A** to this Stipulated Order.

G. Documents Protected from Discovery

1. The production of a privileged or work-product-protected Document, whether inadvertent or otherwise, is not a waiver of privilege or protection from discovery in this case or in any other federal or state proceeding. For example, the mere production of privileged or work-product-protected Documents in this case as part of a mass production is not itself a waiver in this case or in any other federal or state proceeding, in any federal court-mandated arbitration proceeding, or in any foreign proceeding. A Producing Party may assert privilege or protection over produced Documents at any time by notifying the receiving Party in writing of the assertion of privilege or protection regardless of the circumstances under which they were disclosed. Information that contains privileged matter or attorney work product shall be returned immediately if such information appears on its face to the Requesting Party contain such privileged matter or attorney work product if requested by the Producing Party.

2. The Producing Party shall provide the Requesting Party with a log in Excel format of the Documents withheld for privilege containing the information indicated in Federal Rule of Civil Procedure 26(b)(5), including, to the extent reasonably available, the following information: (i) the nature of the privilege (including work product) which is being claimed; (ii) the type of document, *e.g.*, email, letter, or memorandum; (iii) the general subject matter of the document; (iv) the date of the document; and (v) the author of the document, the addressees of the document, and any other recipients, and, where not apparent, the relationship of the author, addressees, and recipients to each other.

3. In-house attorney names shall be designated with a unique ASCII symbol; outside counsel attorney names will be designated with a different unique ASCII symbol. Information to be included in the log may be generated from available Metadata so long as it is reliable and does not contain information that is privileged or protected.

4. Any information required by the log that is itself privileged may be redacted from the log, with the phrase “REDACTED FOR PRIVILEGE” appearing in place of the required information.

5. A single Document containing multiple Email messages (*i.e.*, an Email chain) may be logged as a single entry if the entire chain is privileged. The entry should include sender and recipient information available from the metadata.

6. A Document Family (*e.g.*, an Email and its attachments) may be logged as a single entry so long as the entire Family is privileged and the log entry accurately describes both the Parent and its attachment(s).

7. Activities undertaken in compliance with the duty to preserve information are protected from discovery under Federal Rule of Civil Procedure 26(b)(3).

8. Privilege logs shall be produced within 60 days of the substantial completion of document production.

9. Privileged information produced in this matter will be handled in accordance with Fed. R. Civ. P. 26(b)(5) and Fed. R. Evid. 502.

H. Non-Party Documents

1. A Party that issues a subpoena (“Issuing Party”) upon any non-party shall include a copy of this Order and any protective order agreed and/or entered in this litigation with the subpoena and state that the Parties in this litigation have requested that non-parties produce documents in accordance with the specifications set forth herein, to the extent reasonably feasible.

2. If the Issuing Party receives any Documents in response to a non-party subpoena, the Issuing Party shall produce promptly to all other Parties a copy of the Documents in the form in which they were received and subject to all the procedures and protections set forth in any applicable protective order and may not use those Documents in this Action until such production has been made.

I. Limitation, Non-Waiver and Modification.

1. This Order applies to Documents produced on or after the date this Stipulated Order is fully executed by the Parties.

2. Nothing contained herein is intended to or shall serve to limit a Party’s right to conduct a review of documents, ESI or information (including Metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production.

3. No Producing Party intends to waive (1) any rights, protections or privileged pursuant to confidentiality, attorney-client privilege, attorney work product, United States or foreign data privacy laws, and any other privileges, protections, or objections to discovery, or (2) any objections to the production, discoverability, authenticity, admissibility, or confidentiality of documents and ESI.

4. This Order may be modified by a further Stipulated Order of the Parties or by the Court for good cause shown. Any such modified Stipulated Order will be titled sequentially as follows, “First Modified Stipulated Order Re: Discovery of Electronically Stored Information,” and each modified Stipulated Order will supersede the previous Stipulated Order.

Dated: March 4, 2024

By: /s/ Nicole Gueron

CLARICK GUERON REISBAUM LLP

Nicole Gueron

Isaac B. Zaur

David Kumagai

Katherine Broeksmit

220 Fifth Avenue, 14th Floor

New York, NY 10001

Tel: (212) 633-4310

ngueron@cgr-law.com

izaur@cgr-law.com

dkumagai@cgr-law.com

kbroeksmit@cgr-law.com

*Attorneys for Plaintiff Prophet Mortgage
Opportunities, LP*

Dated: March 4, 2024

By: /s/ Alexander S. Lorenzo

ALSTON & BIRD LLP

Alexander S. Lorenzo
90 Park Avenue
New York, NY 10016
(212) 210-9400
alexander.lorenzo@alston.com

Christopher A. Riley (pro hac vice)
1201 West Peachtree Street NW
Atlanta, Georgia 30309
(404) 881-7000
chris.riley@alston.com

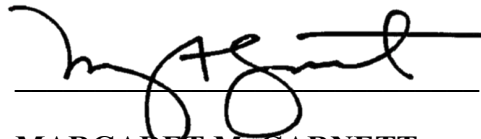
Samuel Bragg (pro hac vice)
Chase Tower
2200 Ross Avenue, Suite 2300
Dallas, TX 75201
(214) 922 3400
sam.bragg@alston.com

Attorneys for Defendants

This Protocol For Discovery Of Electronically Stored Information is hereby APPROVED and ENTERED by this Court. Each Party to this Order is directed to comply with the requirements of this Order.

ORDERED this 11th day of March, 2024.

BY THE COURT

A handwritten signature in black ink, appearing to read 'Margaret M. Garnett', is written over a horizontal line.

MARGARET M. GARNETT
United States District Judge

Exhibit A: Production Format and Table of Metadata Fields

1. Production Deliverable. Productions shall include the following components: Image Files (.TIFF), document level Text Files, an Image Load File (.OPT), a delimited Database Load File containing the metadata fields listed in Section 8 below, and Native Files for Documents produced in Native Format that can be loaded into commercially acceptable production software (e.g. Concordance).

2. Image Files. Except as otherwise provided herein, Documents will be produced in single-page, Group IV, 300 DPI TIFF (1 bit, black & white) images or single-page .JPG (for color images where reasonably requested); along with an .OPT image cross-reference file.

3. Bates Numbering. To the extent possible, Documents and ESI shall be Bates-numbered consecutively maintaining all parent-child relationships. Document numbers for documents produced by the Parties shall identify the Party's name, or an abbreviation of the Party's name, and shall be in the format "Party Name- 00000001.

4. Image Format. Documents produced in Image Format (.TIFF) will be named according to the corresponding Bates numbered images. All Documents that contain comments, deletions and revision marks (including the identity of the person making the deletion or revision and the date and time thereof), speaker notes, or other user-entered data that the source application can display to the user will be processed such that all that data is visible in the image. Each .TIFF will be branded in the lower right-hand corner with its corresponding Bates number, and in the lower left-hand corner with its Confidentiality Designation, if any, using a consistent font type and size. The Bates number and Confidentiality Designation must not obscure any part of the underlying image. If placement of either the Bates number or Confidentiality Designation will result in obscuring the underlying image, the Bates number or Confidentiality Designation should be placed as near to its specified position as possible while preserving the underlying image.

5. Color. Images may be produced in black & white. The Requesting Party may request color images of Documents where color is reasonably necessary to their comprehension or use, and such request shall not unreasonably be denied. Documents produced in color shall be

produced as single-page, 300 DPI JPG images with JPG compression and a high quality setting as to not degrade the original image.

6. Native Format. Files that cannot be converted to image format in a reasonably usable manner, such as spreadsheets (*e.g.*, Excel, Google Sheets), delimited text files (*e.g.*, comma-separated value (.csv) files and tab-separated value (.tsv) files), audio, and video files shall be produced in Native Format unless they require redactions, in which instance the Producing Party will follow the protocol outlined in Section 11 below. A Requesting Party may request the production of other Documents (*e.g.*, PowerPoint presentations) in Native Format where the production of the native file is reasonably necessary to the Document's comprehension or use, and such request shall not unreasonably be denied. For Documents produced in Native Format, a Bates-stamped placeholder in Image Format bearing the legend "This Document has been produced in Native Format" shall also be produced in the same way as any other Image Format Document. Native files shall have a filename that includes the Bates number. Any Party printing the native file for use in this matter shall append and use the placeholder as a cover sheet to the native file at all times. The Parties agree they may use an industry standard native redaction tool for native redactions.

7. Image Load Files. Productions shall include by image load files in Opticon or IPRO format.

8. Database Load Files/Cross-Reference Files. Documents shall be accompanied by a Concordance delimited (*.DAT) load file containing the appropriate link fields and directory information for every file (*e.g.*, image or native files) produced. Load files should include, where the Metadata is reasonably available, the information listed in the Table of Metadata Fields below. The Producing Party is not obligated to populate manually any of the fields below if such fields cannot be extracted from a Document, with the exception of the following: BEGBATES, ENDBATES, BEGATTACH, ENDATTACH, CUSTODIAN, ALLCUSTODIANS, REDACTED, and CONFIDENTIALITY.

Field	Definition	Doc Type
CUSTODIAN	The Custodian (Individual or Source) from whom the documents originated and were deduplicated from	All
ALLCUSTODIANS	All Custodians (Individuals or Sources) whose documents de-duplicated from the original Custodian	All
BEGBATES	Beginning Bates number (production number)	All
ENDBATES	Ending Bates number (production number)	All
BEGATTACH	First Bates number of the first Document in the Document Family	All
ENDATTACH	Last Bates number of the last Document in the Document Family	All
PAGE COUNT	Number of pages in the Document	All
APPLICATION	Commonly associated application for the specified file type	All
NATIVE FILE LINK	The file path for Documents provided in Native Format	All
TEXTPATH	File path for the Searchable Text file	All
PARENT DATE	Date of the Parent Document (mm/dd/yyyy hh:mm:ss AM/PM)	All
HASHVALUE	Hash value (e.g., MD5 or SHA-1)	All
FOLDER	Folder location of the Email within the Native Email application	Email
FROM	Sender	Email
TO	All Recipients that were included on the "To" line of the email	Email
CC	All Recipients that were included on the "CC" line of the email	Email
BCC	All Recipients that were included on the "BCC" line of the email	Email
EMAIL SUBJECT	Subject line of Email	Email
IMPORTANCE	Importance Property of Email (e.g., Normal, Low, High)	Email
DATE/TIME SENT	Date Sent (mm/dd/yyyy hh:mm:ss AM/PM)	Email
DATE/TIME RCVD	Date Received (mm/dd/yyyy hh:mm:ss	Email

Field	Definition	Doc Type
	AM/PM)	
EMAIL TYPE	Type of Email item (e.g., Email, calendar item, contact, note, task)	Email
CONVERSATION ID	Identifier indicating the Email thread to which an Email belongs	Email
FILENAME	Filename from metadata of the Native File at the point of collection	E-Document
FILESIZE	Size of the file	E-Document
TITLE	Title of document or title field extracted from Metadata of non-Email ESI	E-Document
AUTHOR	Any value populated in the Author field of the Document metadata	E-Document
DATE/TIME CREATED	Creation Date (mm/dd/yyyy hh:mm:ss AM/PM)	E-Document
LAST MODIFIED BY	Last person who modified (saved) a Document	E-Document
LAST MODIFIED DATE/TIME	Last Modified Date (mm/dd/yyyy hh:mm:ss AM/PM)	E-Document
E-MESSAGE TYPE	The type of electronic message (e.g., Text Message, Slack, Microsoft Teams, Instant Bloomberg, etc.)	E-Messages
E-MESSAGE PARTICIPANTS	Senders, recipients, subscribers, or others who have the ability to participate in a group message or channel	E-Messages
E-MESSAGE SUBJECT	Subject or name of the messaging thread or topic, if any	E-Messages
LOCATION	Location at which photograph or video was taken	Photos, videos
DOCUMENT TYPE	Descriptor for the type of Document, including: “ Email ” for all Emails; “ E-Message ” for all E-Messages; “ Attachment ” for files that were attachments to Emails or E-Messages; “ Electronic File ” for electronic files not attached to Emails or E-Messages; and “ Hard Copy ” for Hard-Copy Documents	All
PRODVOL	Production volume of data	All
TIMEZONE	Time zone used during processing of data	All

Field	Definition	Doc Type
SOURCE	The Producing Party	All
ATTACHIDS	The IDs of the documents that are attached to the produced document	All
PARENT ID	Indicates the parent ID for an attachment or embedded document. The parent document ID field should be set for all attachments (including attachments that are Emails) but should not be set for parents.	E-Document
MESSAGE ID	The message ID of an Email or other type of electronic message	Email, E-Message
REDACTED	“Yes” should be populated if document contains redaction. (Yes/No format)	All
CONFIDENTIALITY	Field indicating the Confidential treatment of the document.	All

9. Text Files. A single text file containing the Searchable Text as described in Section E.7, *supra*, shall be provided for each Document. The text filename shall be the same as the Bates number of the first page of the Document with the Document extension “.txt” suffixed. Filenames shall not have any special characters or embedded spaces. Searchable Text shall be provided in UTF-8 or Western European (Windows) with Byte Order Mark format text.

10. E-Messages. To the extent E-Messages are produced, a Party will use reasonable efforts to produce such messages such that individual messages are grouped into threads (*i.e.*, continuous conversations between one or more individuals) in a manner to allow for the full context of conversations to be visible.

11. Databases, Structured, Aggregated or Application Data. For requests in which responsive information is contained in a database (*e.g.*, Microsoft Access) or other structured or aggregated data source or otherwise maintained by an application, a Party may produce relevant information by generating one or more reports as done in the ordinary course of business. If the Receiving Party believes that the generation of reports is not adequate, the Parties agree to meet and confer to discuss alternative forms of production. If the Parties cannot reach agreement, the matter may be submitted to the Court for resolution.

12. Redactions. The Parties may redact from any TIFF image, metadata field, or native file information that is (1) privileged or protected from discovery as work product or by reason of any other applicable privilege or immunity; or (2) protected personal information (*e.g.*, credit card numbers, account passwords, SSNs) subject to non-disclosure obligations imposed by governmental authorities, law, or regulation. Subject to the limitations herein, no redactions may be made.

- a. Native Files that require redaction may be produced in either redacted TIFF or as a native redacted using and industry standard tool with searchable OCR text so long as it is comprehensible and similarly usable to the unredacted Document. A Requesting Party may request the re-production of a redacted Native File where such production is reasonably necessary to the Document's comprehension or use, and such request shall not unreasonably be denied.
- b. Redacted documents will be produced with the associated metadata for the document, to the extent possible without compromising the privileged or protected information. Redacted Documents shall be identified as such in the Metadata fields Redacted and Redaction Basis.
- c. Attachments to Emails or other Documents whose entire contents can be redacted may be produced as slip-sheets stating that the attachment has been redacted in full. Slip-sheets shall be in the same position in the family as if the withheld Documents had been produced. Email header information (*e.g.*, date, subject line, etc.) should not be redacted unless it is independently privileged.

13. Document Families. The Parties agree to produce documents responsive to a Party's documents requests, family complete, with the exception of slip-sheeting documents withheld entirely on a claim of privilege.

14. Foreign Language Documents. All documents shall be produced in their original language. Where a requested document exists in a foreign language and the Producing Party also

has an English-language version of that document that it prepared for non-litigation purposes prior to filing of the lawsuit, the Producing Party shall produce both the original Document and all English-language versions. Nothing in this Order shall require a Producing Party to prepare a translation, certified or otherwise, for foreign language documents that are produced in discovery.

15. Re-productions. Notwithstanding any provisions to the contrary, Documents that the Producing Party re-produces in whole or in part from the production files of another litigation, arbitration, government inquiry, or other matter may be produced in the same manner and form as originally produced in the other matter, provided that a Party will re-produce documents in a different format for good cause shown.

16. Replacement Productions. Any replacement production will be transmitted with a cover letter or Email to identify the production as a replacement and cross-reference the BegDoc and EndDoc of the Documents being replaced. Replacement productions shall include load files necessary to link the replacement file to other previously produced document family members. If the replacement production is being transmitted by physical media, the media shall include the phrase “Replacement Production.”

17. Production Media. The Producing Party will provide the production data via high speed secure FTP site, electronic media (encrypted hard drive or thumb drive,), or by way of other electronic transfer, as between accounts at a cloud provider (subject to prior agreement with the Requesting Party) (“Production Media”). The Producing Party shall encrypt or password protect the production data, and the Producing Party shall forward the password to decrypt the production data separately from the SFTP site or electronic media to which the production data is saved. Prior to a Producing Party’s initial production, the Producing Party shall seek from the Requesting Party the relevant contact information of the individuals to receive the Production Media and passwords. Each piece of Production Media shall identify: (1) the Producing Party’s name; (2) a production number corresponding to the production volume (*e.g.*, “VOL001,” “VOL002”), as well as the volume of the material in the production (*e.g.*, “-001,” “-002”); (3) the production date; and (4) the Bates Number range of the materials contained on the Production Media.